

European Patent Office

Publication Number: EP 0 464 320 A2

EUROPEAN PATENT APPLICATION

Application Number: 91105666.1

Int. Cl.⁵: G06F 1/00

Application Date: 10 April 91

Priority: 6 July 90 DE 4021535

Publication Date of Application:
8 January 92 Patentblatt 92/02

Named Convention States:
AT BE CH DE DK ES FR GB
GR IT LI LU NL SE

Applicant: GIGATAPE SYSTEME FUER
DATENSICHERUNG GMBH
Benzstrasse 28
W-8039 Puchheim(DE)

Inventor: Brauner, Ingolf
Schützenstrasse 15
W-8912 Kaufering(DE)

Representative: Weber, Otto Ernst, Dipl.-Phys. et al.
Weber & Heim Hofbrunnstrasse 36
W-8000 München 71(DE)

Method for generating individual data medium protection against unauthorized use

A method is described for generating individual protection of a data medium, for example a magnetic tape cassette, against unauthorized use in a data processing device. The protection prevents a data processing program contained on the data medium from being used or copied without authorization. For this purpose at the manufacturer end a device-specific identification, for example a device serial number, is preferably automatically scanned and stored at the device end. As soon as a data medium is placed for the first time into the device, it writes the identification onto the data medium. From this time on this data medium can only be accessed with this device.

AK PF 980072

CITED BY APPLICANT

THIS PAGE BLANK (USPTO)

The invention relates to a method for generating individual protection of a data medium, for example a magnetic tape cassette, using a device identification against unauthorized use in a data processing device.

It is known that the unauthorized use and/or copying of data processing programs, also referred to as program piracy, is a serious economic problem for the program manufacturer. If the use and multiplication outside of the domain of influence of the manufacturer can take place without any controls, appropriate economic utilization is no longer possible. To prevent pirated copies and unauthorized software use, therefore a number of mechanical and program-controlled security measures has been employed. One known method comprises permitting the use of a program data medium only in a specific data processing device and to prevent the program from executing in any other device. This takes place with the aid of an additional coding unit, which, for example is accommodated on a plug-in card or a so-called dongle. While therewith the desired great protection against unauthorized users is attained, through the pairwise assignment of coding unit and data medium, a relatively large storage and management expenditure is required at the manufacturer and dealer end since the dealer must have available for each coding unit the associated data media and must ensure that no mistaken interchange occurs.

The invention is based on the task of specifying a method of the above described type, which ensures great protection and simultaneously can be reduced to practice with low expenditures.

This task is solved thereby that the device identification is stored by the manufacturer in the data processing device, that at the initial use of the particular data medium in this device the device identification is written onto the data medium and that at the user end, the device and data medium identification is automatically checked for agreement.

THIS PAGE BLANK (USPTO)

This entails the advantage that the program manufacturer can produce and market all data media identically, i.e. a fixed assignment between a data medium and a data processing device is initially not required. Storekeeping and administration is therefore considerably simplified. This applies also to the distribution channels, where the number of data media that must be kept on hand with respect to different devices can be relatively small. It is only when the distributor or end user has placed a legitimately obtained data medium for the first time into his device, is it marked as being specific to this device. From this time on the data medium can only and exclusively be used in this device. Expressed differently, this means that the unique assignment of device and data medium takes place only in the last step of the distribution channel or by the end user, with the device itself replacing the so-called dongle.

A further advantage lies therein that in the event of a device repair and/or when replacing components of the device, the original identification can be taken over in simple manner such that the already available coded data media can continue to be used.

The invention also has the great advantage that security copies of the marked data media can be produced in any desired number without the desired protection being restricted.

Further the method can be combined in simple manner with function and/or quality tests, which are carried out at the manufacturer end before the device is delivered. Subsequently the control processor, which is provided in any event, can be utilized for reading and storing the device identification.

Reading-in the device identification is especially simple if it is applied on the device such that it is machine readable, since in this case a high degree of automatization is attained. However, in principle it is also possible for the device identification to be entered by an operating person, for example through a keyboard.

A preferred development comprises that the device identification consists of a bar code, which is adhered on the device which can also be evaluated in a different manner, for example in connection with the storekeeping and the like.

THIS PAGE BLANK (USPTO)

The method can be implemented especially simply if, as the device identification, the serial number of the device is utilized, since it is present on the device in any event.

Through a corresponding selection of the device identification and/or of further labels, in a preferred development of the invention it is possible to identify data media such that they can be used in a predetermined number of data processing devices. This has the advantage that, for example, data media can be generated which can be employed for service purposes to a predetermined extent without the device-specific protection becoming effective in every case.

In addition, the option is provided that while the appropriately labeled data media can be exchanged and used within a set of devices of a user, their use outside of this set of devices is impossible.

In the following the invention will be described in conjunction with an embodiment example depicted in the drawing.

The configuration illustrated in the Figure comprises a control processor 10, such as is used, for example, in automatic production test systems for a data processing device 11. The functions of the data processing device 11 are checked with the control processor 10 in known manner at the manufacturer end before it is delivered to the trade or to the end user. The data exchange takes place across connection lines 12.

On the housing of the data processing device 11 is applied a machine-readable device identification 13, which, in the example shown, consists of a bar code comprising a device serial number. With the aid of a reader 14 the device identification is read automatically by the control of the control processor 10 and from there is automatically transferred into the data processing device and stored at the device end. The storage takes place in a rewritable read-only memory, for example an EEPROM or a programmable logic, for example EPLD. In the present example reading and transferring the device identification 13 is carried out during the automatically proceeding function tests.

If, at a later point in time, a data medium provided with a program, such as

THIS PAGE BLANK (USPTO)

for example a magnetic tape cassette or a floppy disk, is placed initially into the data processing device, the latter - without the user having any influence over it - writes the stored device identification onto the data medium and in this way, establishes a unique assignment. Data media, which are not provided with this individual device-specific identification and, instead, have a different identification, are rejected by this data processing device 13 as being impermissible and only the use of data media is possible which were provided with the device identification.

THIS PAGE BLANK (USPTO)



Europäisches Patentamt
European Patent Office
Office européen des brevets



Veröffentlichungsnummer: **0 464 320 A2**

EUROPÄISCHE PATENTANMELDUNG

Anmeldenummer: **91105666.1**

Int. Cl.⁵: **G06F 1/00**

Anmeldetag: **10.04.91**

Priorität: **06.07.90 DE 4021535**

Veröffentlichungstag der Anmeldung:
08.01.92 Patentblatt 92/02

Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

Anmelder: **GIGATAPE SYSTEME FUER
DATENSICHERUNG GMBH
Benzstrasse 28
W-8039 Puchheim(DE)**

Erfinder: **Brauner, Ingolf
Schützenstrasse 15
W-8912 Kaufering(DE)**

Vertreter: **Weber, Otto Ernst, Dipl.-Phys. et al
Weber & Helm Hofbrunnstrasse 36
W-8000 München 71(DE)**

Verfahren zum Erzeugen eines individuellen Datenträgerschutzes gegen eine unautorisierte Benutzung.

Es wird ein Verfahren zum Erzeugen eines individuellen Schutzes eines Datenträgers, beispielsweise einer Magnetbandkassette, gegen eine unautorisierte Benutzung in einem Datenverarbeitungsgerät beschrieben. Der Schutz verhindert, daß ein auf dem Datenträger enthaltenes Datenverarbeitungsprogramm unautorisiert benutzt oder kopiert wird. Zu diesem Zweck wird herstellerseitig eine gerätespezifische Kennzeichnung, beispielsweise eine Geräteseriennummer, bevorzugt automatisch abgetastet und geräteseitig abgespeichert. Sobald ein Datenträger in das Gerät erstmalig eingelegt wird, schreibt dieses die Kennzeichnung auf den Datenträger. Von diesem Zeitpunkt an kann auf den Datenträger nur mit diesem Gerät zugegriffen werden.

Die Erfindung betrifft ein Verfahren zum Erzeugen eines individuellen Schutzes eines Datenträgers, beispielsweise eine Magnetbandkassette, gegen eine unautorisierte Benutzung in einem Datenverarbeitungsgerät unter Verwendung einer Gerätekennzeichnung.

Bekanntlich ist das unautorisierte Benutzen und/oder Kopieren von Datenverarbeitungsprogrammen, das auch als Programmpiraterie bezeichnet wird, ein großes wirtschaftliches Problem für die Programmhersteller. Wenn die Benutzung und Vervielfältigung außerhalb des Einflusses des Herstellers unkontrolliert erfolgen kann, ist eine angemessene wirtschaftliche Verwertung nicht mehr möglich. Zur Verhinderung von Raubkopien und unberechtigten Software-Benutzungen wurde daher eine Reihe von mechanischen und programmgesteuerten Sicherheitsvorkehrungen getroffen. Ein bekanntes Verfahren besteht darin, die Benutzung eines Programmdatenträgers nur in einem bestimmten Datenverarbeitungsgerät zu gestatten und bei jedem anderen Gerät einen Programmablauf zu verhindern. Dies erfolgt mit Hilfe einer zusätzlichen Kodiereinheit, die beispielsweise auf einer Steckkarte oder einem sogenannten Dongle untergebracht ist. Es wird damit zwar der erwünschte große Schutz gegen unberechtigte Benutzer erreicht, andererseits ist durch die paarweise Zuordnung von Kodiereinheit und Datenträger hersteller- und händlerseitig ein relativ großer Lager- und Verwaltungsaufwand erforderlich, weil der Händler zu jeder Kodiereinheit die zugehörigen Datenträger bereithalten und darauf achten muß, daß keine Vertauschung stattfindet.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren der eingangs genannten Art anzugeben, welches einen großen Schutz gewährleistet und gleichzeitig mit geringem Aufwand praktikierbar ist.

Diese Aufgabe wird dadurch gelöst, daß die Gerätekennzeichnung herstellerseitig im Datenverarbeitungsgerät gespeichert wird, daß beim erstmaligen Benutzen des betreffenden Datenträgers in diesem Gerät die Gerätekennzeichnung auf den Datenträger geschrieben wird, und daß benutzerseitig selbsttätig die Geräte- und Datenträgerkennzeichnung auf Übereinstimmung überprüft werden.

Das hat den Vorteil, daß der Programmhersteller alle Datenträger identisch herstellen und vermarkten kann, d.h. eine feste Zuordnung zwischen einem Datenträger und einem Datenverarbeitungsgerät ist zunächst nicht erforderlich. Die Lagerhaltung und Verwaltung wird daher beträchtlich vereinfacht. Dies gilt auch für die Vertriebswege, wo die Anzahl der bereitzuhaltenden Datenträger in Bezug auf verschiedene Geräte relativ klein sein kann. Erst wenn der Vertreiber oder Endbenutzer einen rechtmäßig erworbenen Datenträger erstmalig in sein Gerät eingelegt hat, wird dieser geräte-

spezifisch gekennzeichnet. Von diesem Zeitpunkt an kann der Datenträger ausschließlich in diesem Gerät benutzt werden. Anders ausgedrückt bedeutet dies, daß die eindeutige Zuordnung von Gerät und Datenträger erst in der letzten Stufe des Vertriebsweges bzw. beim Endbenutzer erfolgt, wobei das Gerät selbst den sogenannten Dongle ersetzt.

Ein weiterer Vorteil ist darin zu sehen, daß im Falle einer Gerätereparatur und/oder bei einem Bauteile austausch des Geräts die ursprüngliche Kennzeichnung auf einfache Weise übernommen werden kann, so daß die bereits vorhandenen, codierten Datenträger weiterverwendet werden können.

Die Erfindung hat auch den großen Vorteil, daß Sicherungskopien der gekennzeichneten Datenträger in beliebiger Anzahl angefertigt werden können, ohne daß der erwünschte Schutz eingeschränkt wird.

Ferner ist das Verfahren auf einfache Weise mit Funktions- und/oder Qualitätstests kombinierbar, die herstellerseitig vor der Geräteauslieferung vorgenommen werden. Es kann dann zum Lesen und Abspeichern der Gerätekennzeichnung der ohnehin vorhandene Steuerrechner herangezogen werden.

Das Einlesen der Gerätekennzeichnung ist besonders einfach, wenn sie auf dem Gerät maschinenlesbar angebracht ist, weil dann ein hoher Automatisierungsgrad erreicht wird. Grundsätzlich ist es jedoch auch möglich, die Gerätekennzeichnung von einer Bedienperson, beispielsweise über eine Tastatur, einzugeben.

Eine bevorzugte Ausgestaltung besteht hierbei darin, daß die Gerätekennzeichnung aus einem Barcode besteht, der auf das Gerät aufgeklebt ist, der auch in anderer Weise, beispielsweise im Zusammenhang mit der Lagerverwaltung und ähnlichem ausgewertet werden kann.

Besonders einfach kann das Verfahren durchgeführt werden, wenn als Gerätekennzeichnung die Geräteseriennummer verwendet wird, weil sie ohnehin an jedem Gerät vorhanden ist.

Durch eine entsprechende Wahl der Gerätekennzeichnung und/oder von weiteren Kennzeichnungen ist es in einer bevorzugten Ausgestaltung der Erfindung möglich, Datenträger in der Weise zu kennzeichnen, daß sie in einer vorgegebenen Anzahl von Datenverarbeitungsgeräten benutzt werden können. Das hat den Vorteil, daß beispielsweise Datenträger erzeugt werden können, die für Servicezwecke in einem vorgegebenen Umfang eingesetzt werden können, ohne daß der gerätespezifische Schutz in jedem Fall wirksam wird.

Es wird damit ferner die Möglichkeit geschaffen, daß die entsprechend gekennzeichneten Datenträger zwar innerhalb einer Gerätemenge eines Anwenders ausgetauscht und benutzt werden kön-

nen, daß aber eine Verwendung außerhalb dieser Gerätemenge ausgeschlossen ist.

Nachfolgend wird die Erfindung anhand eines in der Zeichnung dargestellten Ausführungsbeispiels weiter beschrieben.

Die in der Figur veranschaulichte Konfiguration umfaßt einen Steuerrechner 10, wie er beispielsweise in automatischen Produktionstestsystemen für ein Datenverarbeitungsgerät 11 verwendet wird. Mit dem Steuerrechner 10 werden auf bekannte Weise herstellereitig die Funktionen des Datenverarbeitungsgeräts 11 überprüft, bevor es in den Handel oder an Endverbraucher ausgeliefert wird. Der Datenaustausch erfolgt über Verbindungsleitungen 12.

Auf dem Gehäuse des Datenverarbeitungsgeräts 11 ist eine maschinenlesbare Gerätekennzeichnung 13 angebracht, die im dargestellten Beispiel aus einem eine Geräteseriennummer enthaltenden Barcode besteht. Mit Hilfe eines Lesers 14 wird die Gerätekennzeichnung von der Steuerung des Steuerrechners 10 automatisch gelesen und von dort selbsttätig in das Datenverarbeitungsgerät übertragen und geräteseitig gespeichert. Die Speicherung erfolgt in einem wiederbeschreibbaren Festwertspeicher, z.B. einem EEPROM, oder einer programmierbaren Logik, z.B. EPLD. Das Lesen und Übertragen der Gerätekennzeichnung 13 wird im vorliegenden Beispiel während der automatisch ablaufenden Funktionstests durchgeführt.

Wird zu einem späteren Zeitpunkt ein mit einem Programm versehener Datenträger, wie beispielsweise eine Magnetbandkassette oder eine Floppy-Disk, in das Datenverarbeitungsgerät erstmalig eingelegt, so schreibt dieses - ohne daß der Benutzer darauf Einfluß hat - die abgespeicherte Gerätekennzeichnung auf den Datenträger und stellt auf diese Weise eine eindeutige Zuordnung her. Datenträger, die nicht mit dieser individuellen, gerätespezifischen Kennzeichnung versehen sind und stattdessen eine andere Kennzeichnung aufweisen, werden von diesem Datenverarbeitungsgerät 13 als unzulässig zurückgewiesen und es ist ausschließlich die Benutzung von Datenträgern möglich, die mit der Gerätekennzeichnung versehen wurden.

Patentansprüche

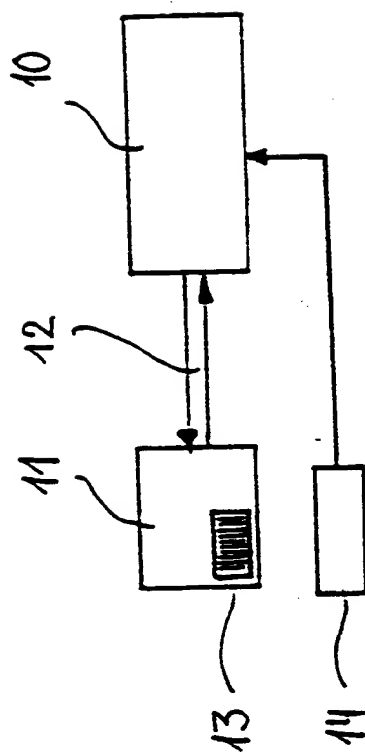
1. Verfahren zum Erzeugen eines individuellen Schutzes eines Datenträgers, beispielsweise einer Magnetbandkassette, gegen eine unautorisierte Benutzung in einem Datenverarbeitungsgerät unter Verwendung einer Gerätekennzeichnung, **gekennzeichnet** durch folgende Verfahrensschritte:
(a) Herstellerseitiges Abspeichern der Gerä-

tekennzeichnung in einem geräteseitigen Speicher

(b) Schreiben und Abspeichern der Gerätekennzeichnung auf den/dem Datenträger(n) beim erstmaligen Benutzen im betreffenden Datenverarbeitungsgerät

(c) Benutzerseitiges, selbsttätiges Überprüfen der Geräte- und Datenträgerkennzeichnung auf Übereinstimmung.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß auf dem Datenverarbeitungsgerät herstellereitig eine maschinenlesbare Gerätekennzeichnung angebracht wird und daß sie maschinell gelesen wird.
3. Verfahren nach Anspruch 1 oder 2, dadurch **gekennzeichnet**, daß das Lesen und Abspeichern der Gerätekennzeichnung unter Kontrolle eines Steuerrechners durchgeführt wird, der zusätzlich Funktions- und/oder Qualitätstests für das betreffende Datenverarbeitungsgerät steuert.
4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß weitere Kennzeichnungen eingelesen, abgespeichert und gegebenenfalls auf einen Datenträger geschrieben werden, welche eine Benutzung des Datenträgers in mehreren Datenverarbeitungsgeräten gestatten.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch **gekennzeichnet**, daß als Gerätekennzeichnung eine Geräteseriennummer verwendet wird.





Europäisches Patentamt
European Patent Office
Office européen des brevets



Veröffentlichungsnummer: **0 464 320 A3**

12

EUROPÄISCHE PATENTANMELDUNG

21 Anmeldenummer: **91105666.1**

51 Int. Cl. 5: **G06F 1/00**

22 Anmeldetag: **10.04.91**

30 Priorität: **06.07.90 DE 4021535**

43 Veröffentlichungstag der Anmeldung:
08.01.92 Patentblatt 92/02

84 Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

88 Veröffentlichungstag des später veröffentlichten
Recherchenberichts: **05.08.92 Patentblatt 92/32**

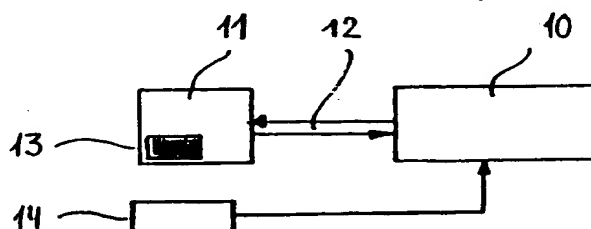
71 Anmelder: **GIGATAPE SYSTEME FUER
DATENSICHERUNG GMBH
Benzstrasse 28
W-8039 Puchheim(DE)**

72 Erfinder: **Brauner, Ingolf
Schützenstrasse 15
W-8912 Kaufering(DE)**

74 Vertreter: **Weber, Otto Ernst, Dipl.-Phys. et al
Weber & Heim Hofbrunnstrasse 36
W-8000 München 71(DE)**

54 Verfahren zum Erzeugen eines individuellen Datenträgerschutzes gegen eine unautorisierte Benutzung.

57 Es wird ein Verfahren zum Erzeugen eines individuellen Schutzes eines Datenträgers, beispielsweise einer Magnetbandkassette, gegen eine unautorisierte Benutzung in einem Datenverarbeitungsgerät beschrieben. Der Schutz verhindert, daß ein auf dem Datenträger enthaltenes Datenverarbeitungsprogramm unautorisiert benutzt oder kopiert wird. Zu diesem Zweck wird herstellerseitig eine gerätespezifische Kennzeichnung, beispielsweise eine Geräteseriennummer, bevorzugt automatisch abgetastet und geräteseitig abgespeichert. Sobald ein Datenträger in das Gerät erstmalig eingelegt wird, schreibt dieses die Kennzeichnung auf den Datenträger. Von diesem Zeitpunkt an kann auf den Datenträger nur mit diesem Gerät zugegriffen werden.



EP 0 464 320 A3



Europäisches
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung

EP 91 10 5666

| EINSCHLÄGIGE DOKUMENTE | | | |
|--|--|---|--|
| Kategorie | Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile | Betrifft Anspruch | KLASSIFIKATION DER ANMELDUNG (Int. Cl.5) |
| Y | US-A-4 891 504 (GUPTA) * Abbildungen 1,3,4 * * Spalte 2, Zeile 21 - Zeile 33 * * Spalte 4, Zeile 36 - Zeile 45 * | 1,2,4 | G06F1/00 |
| Y | IBM TECHNICAL DISCLOSURE BULLETIN, Bd. 21, Nr. 2, Juli 1978, NEW YORK US Seiten 836 - 837; A. GURUGE: 'PREVENTING UNAUTHORIZED ACCESS TO DISKETTE -LOADED MICROCODE' * das ganze Dokument * | 1,2,4 | |
| | | | RECHERCHIERTE SACHGEBIETE (Int. Cl.5) |
| | | | G06F |
| Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt | | | |
| Recherchant DEN HAAG | | Abschlußdatum der Recherche 09 JUNI 1992 | Prüfer WEISS P. |
| KATEGORIE DER GENANNTEN DOKUMENTE | | | |
| X : von besonderer Bedeutung als als betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : mündliche Offenbarung P : Zwischenliteratur | | | |
| T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldetermin veröffentlicht worden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument A : Mitglied der gleichen Patentfamilie, überlappendes Dokument | | | |

EPO FORM 153 (12/81) (7/82)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)